24th Annual
SSTC
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

The New Agile Systems Engineering: Meeting the Challenges of Functionality, Security, and Austerity

4-24-2012

Dr. Bassam Farroha
Technical Director
IA Architecture and Applications Office
Department of Defense
bassam.s.farroha@ugov.gov

Ms. Deborah L. Farroha
Technical Director
Enterprise Systems Engineering and Architecture
Department of Defense
Deborah.l.Farroha@ugov.gov

24th Annual
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

Agenda

- Introduction to Problem Space
  - Agility is key
- Drivers
  - Enterprise Information Sharing
  - Securing Interactions
  - Crossing Security Domains
  - Security Via Commercial Solutions
- Service Based Architecture and Systems Engineering
- Data as a Service
- Framework for the Agile Secure Service Based Architecture

Introduction

- This research investigated **methods and environments to deliver capabilities** for secure information analysis, processing and sharing
  - On time—through Corporate Services
  - Securely—leveraging the tenets of IA
  - **Balance** between **sharing** data and **protecting** data and environment
- Defined the Enterprise **boundary**
  - Composed of **System of Systems (SoS)**
  - **Snap shot in time**
  - **Adapt** to continuously **changing boundary**—facilitated by **Agile Development**
- **Resulting Framework has to be flexible** to accommodate changes in policies and threats
  - **Agile** development
  - **Continuously asses new threats** and investigate **technologies** to counter them
  - **Incremental** fielding of **Services**

24th Annual
SSTC
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

The Cloud…

- **Moving data, services and apps to the Cloud…**
  - Is an enabler to Agile Development:
    - Provides an ad-hoc ability to provision a development environment "on the fly" with operational surroundings
    - Postured for quick deployment given the access to data, users and services
    - Enables a dynamic operational environment that adapts to the needs of the users or systems "in the cloud"
  - Provides the ability to gain efficiencies through consolidation and virtual access (i.e. network enclave removal, power, space, cooling, processing, etc)
  - Creates an environment where access control is paramount to data sharing, data protection and Information Security
    - Obliges us to seriously consider Risk Adaptive Attribute-based access control (RAdAC)
    - Compels us to look at Policy-based routing

Securing the Cloud

- Traditional Defense Strategy
  - External Threats
  - Internal Threats
  - Boundary
- New Approach:
  - Labeling Data (Crypto-Bound Metadata)
  - Smart Data
  - Positive control on Identity and Access
  - Secure Configuration
  - Layered Security….Roots of Trust
  - Fine Grain Access Control
  - Network Management
  - Real Time Monitoring
- Multi Level Security

Commercial Solution For Sensitive and Classified

- Why Commercial Products and Services
  - Time to Market
  - Cost
  - Adaptation
  - Interoperability
  - Working with Coalition
  - Upgradeability
  - Layered security
  - Main tenability
  - Expandability
  - Reduction in training costs
- Why Not Commercial
  - Own the design process and can change requirements any time
  - Build in as much native security
  - Reduce insider threat and backdoor
  - Special situations where commercial is unacceptable due to mission impact
  - supply chain Risk management

Secure Mobile

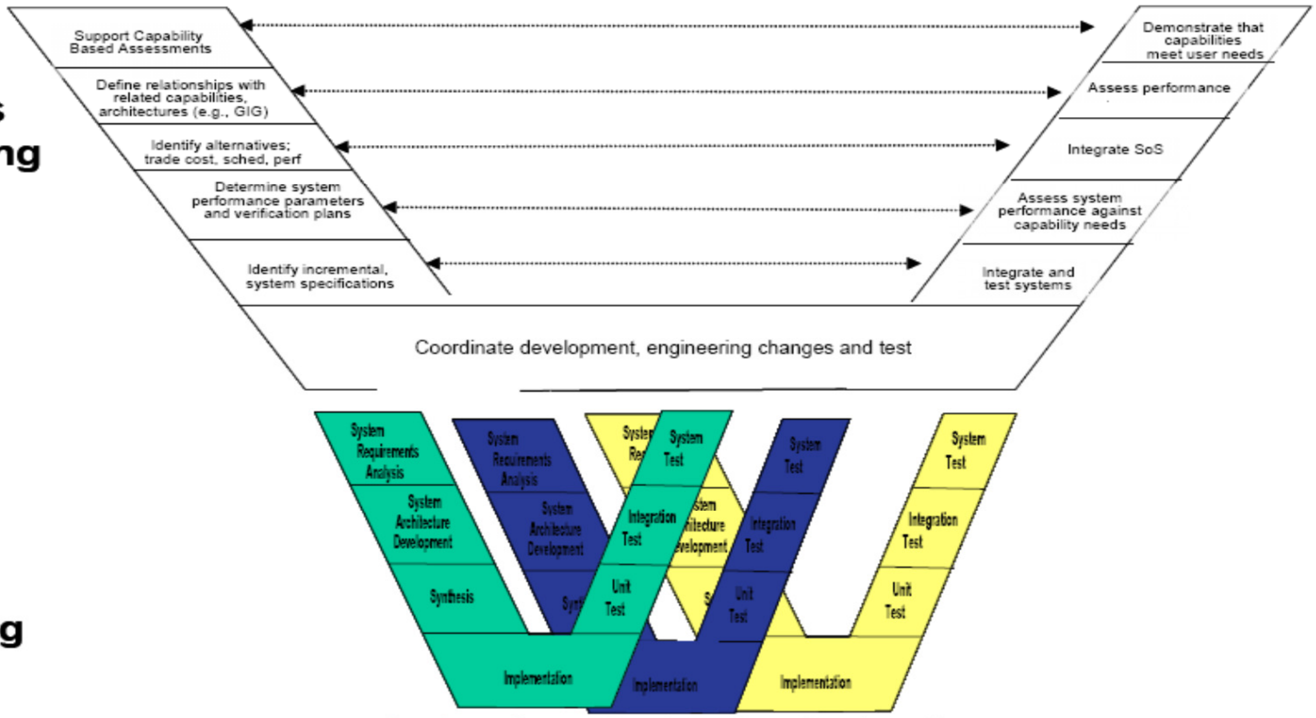
- **Corporate Mobile Device**
  - Use trusted Operating Systems
  - Utilize Corporate Security Policy
  - Corporate controls on Accessible sites
  - Need to automate policy and ***develop agile provisioning strategy***
- **Personal Device for dual use**
  - Dual boot device
  - Corporate has access to onboard corporate data only
  - If corporate security policy is disabled, access to the enterprise is terminated
  - Corporate data rights stay with the corporation
  - *Agile Real-Time Monitoring*
    - Monitor device integrity
    - Monitor vendor (service provider) upgrades to OS and Apps
    - Monitor user updates and APPs

System of Systems (SoS) and Enterprise Systems Engineering

For Each Increment

SoS Systems Engineering

Service/ PEO/PM Program Systems Engineering


Support Capability Based Assessments
Define relationships with related capabilities, architectures (e.g., GIG)
Identify alternatives; trade cost, sched, perf
Determine system performance parameters and verification plans
Identify incremental, system specifications
Demonstrate that capabilities meet user needs
Assess performance
Integrate SoS
Assess system performance against capability needs
Integrate and test systems
Coordinate development, engineering changes and test
System Requirements Analysis
System Architecture Development
Synthesis
Implementation
Unit Test
Integration Test
System Test
System Requirements Analysis
System Architecture Development
Synt
Implementation
Unit Test
Integration Test
System Test
System Re
stem hitecture evelopment
S
Implementation
Unit Test
Integration Test
System Test

System 1 (Requiring Modification)

System 2 (New or Early in Development)

System 3 (In production)

Adaptive Systems Engineering…

- **What about Systems Engineering?**
  - **SE is most relevant at the early stages of development**
    - **Define Interfaces**
    - **Characterize Data Flow (mission data to netflow data)**
    - **Define Thresholds for proactive fine-tuning of system attributes (metrics monitoring, smart trending, etc)**
    - **Develop the sustainability concept of operations**
    - **Identify the risks and vulnerabilities**
    - **Enable fault isolation through identification of high risk components**
  - **Create repeatable processes that <u>add value</u>**
    - **Generate a lean governance practice that enables the ability to recognize the baseline**
    - **Define a regression testing process to "quickly" test the new capability**
  - **SE must be ADAPTIVE to be RELAVENT**
    - **Understand the criticality of the need**
    - **Understand the timeline**
    - **Evaluate the changing threat Environment**
    - **Understand your stakeholder and operational environment**

Objectives for the Cyber Security Framework

- **Ubiquitous Application:**
  - We need a solution that is **generally applicable to all systems**, non-virtualized and virtualized.
- **Just-in-time Delivery:**
  - Time and effort must be **predictable** otherwise we could lose sight of our end goal by continuing to develop without any perceived deadline or end-point.
  - Continuous evaluation of current COTS , Commercial offerings, and the Technology pipeline
- **Pervasive C&A:**
  - **Streamline** the Certification & Accreditation (C&A) process to be able to provision capabilities that use "C&A" compliant services to enable shorter delivery times.
  - **Reciprocity** Across user Community
- **Service Interface Attributes:**
  - Need to be **well defined** for other apps to leverage **expedite development**, certification, accreditation, and deployment processes.
  - Standardize interfaces
- **Define a Framework that includes:**
  - A **native governance** mechanism
  - The **ability to illuminate the gaps** in technology/capability
  - The **authority to allow for a prioritization** of resources to focus on the most important mission needs.
  - An Enterprise **Services taxonomy** so that shows ***what services align to what mission element***

What does it mean to be Agile?

- Being agile is not only a state of being, but a ***mind-set*** that **bridges customers' expectations** to **developers' techniques**.
- **Agile** development teams **respond** to the **instability of requirements** through an incremental, iterative work tempo.
  - Sprints
  - Spins
  - Iterations
- The DoD is moving away from the Waterfall method because:
  - **Unpredictable** threat environment
  - The need to **deliver** capability in **months** not years
- Agile methods are ***adaptive*** *rather than* ***predictive***
  - Refactoring/Refinement allows for customized **early capability delivery**
  - Philosophy….."Build a little, Test a little, ***Deploy a little***"
  - Develop mitigation techniques to deal with Attacks through Agile Adaptive processes

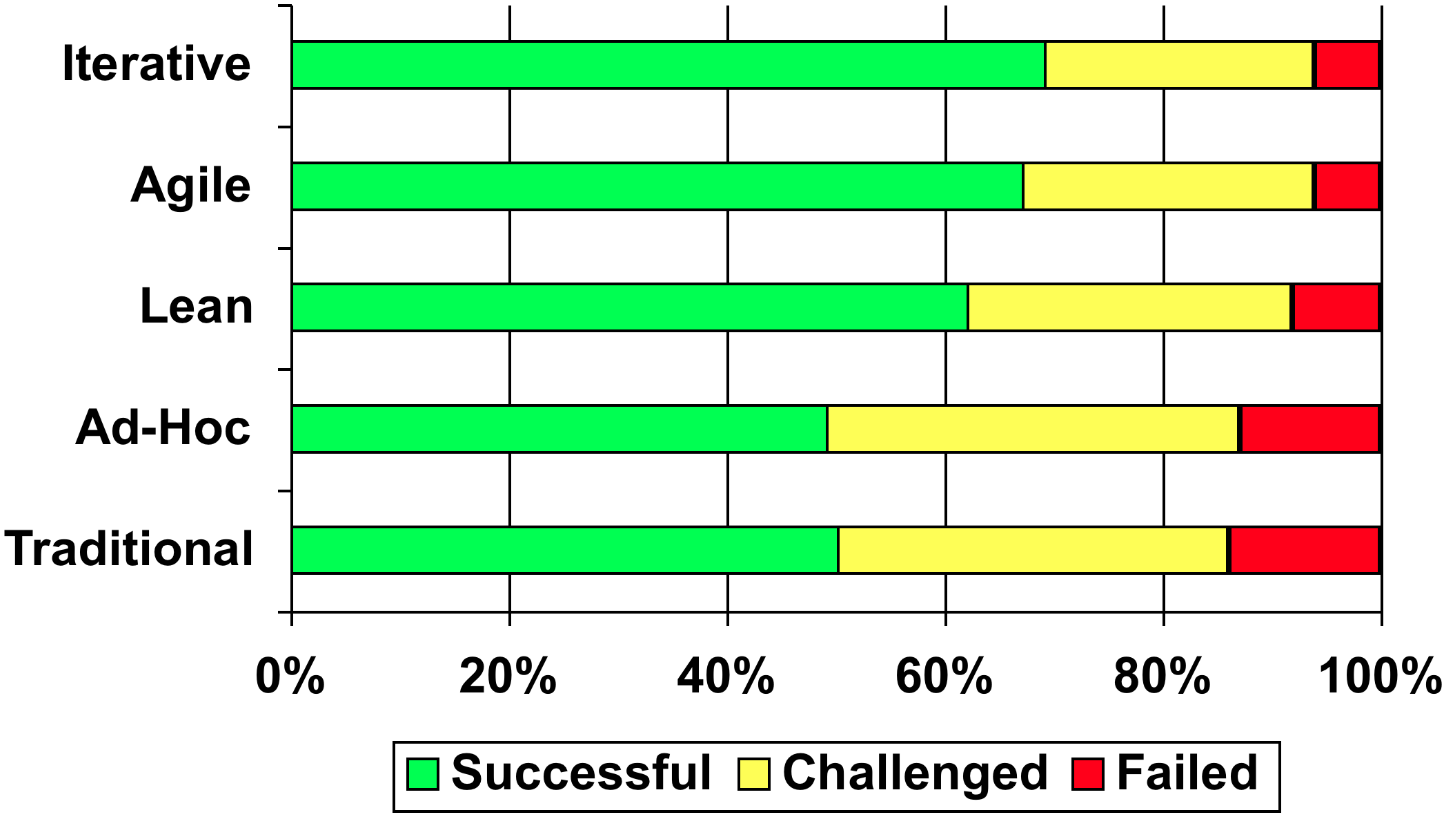
24th Annual
SSTC
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

5 Tenets of Agile

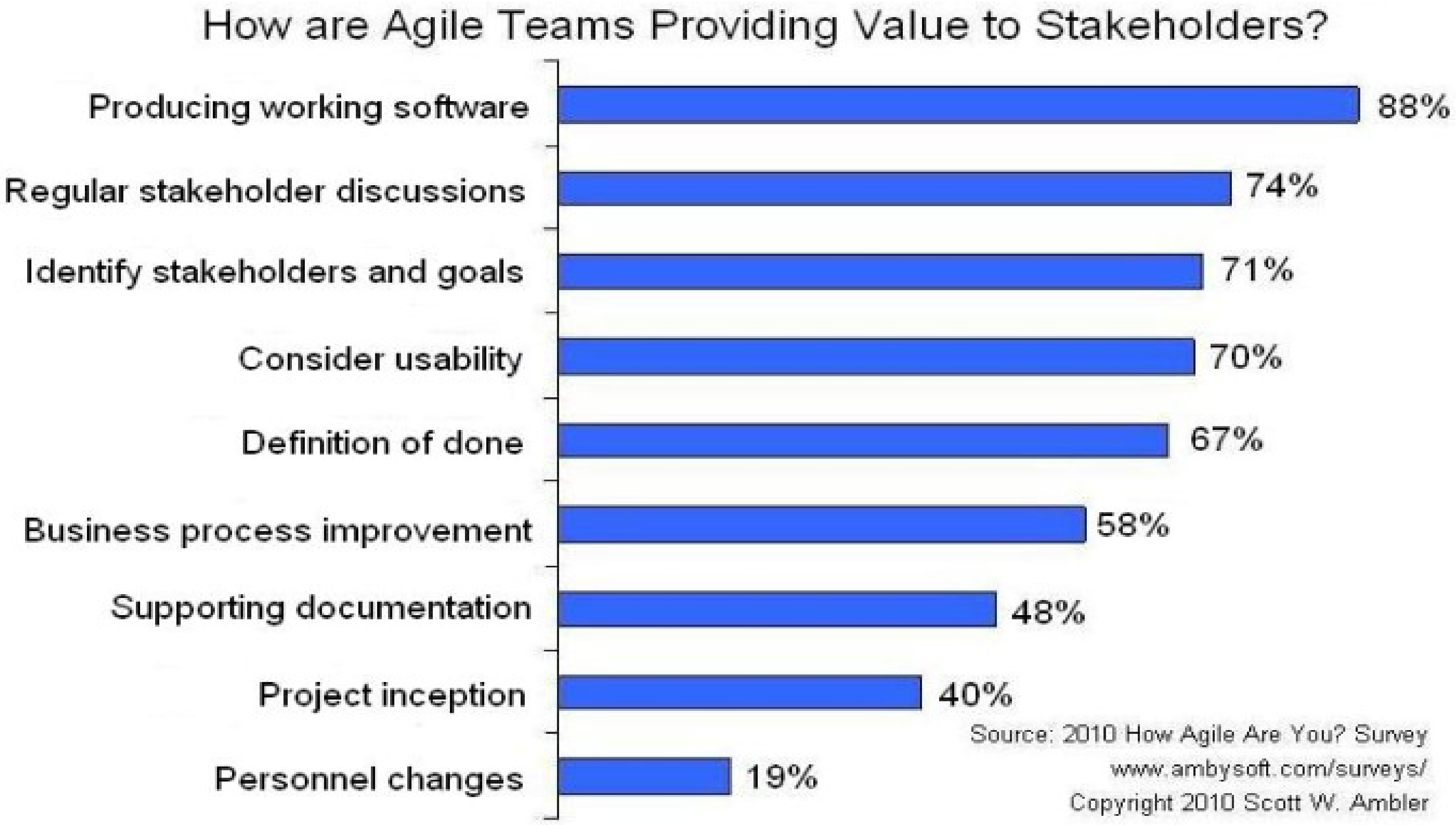
- **Value:** Produce a consumable solution on a regular basis which provides value to stakeholders.
- **Validation:** Do continuous regression testing, and better yet take a Test-Driven Development (TDD) approach.
- **Stakeholders:** Work closely with their stakeholders, or a stakeholder proxy, ideally on a daily basis.
- **Self-organization:** Are self-organizing and work within an appropriate governance framework.
- **Improvement:** Regularly reflect on, and measure, how they work together and then act to improve on their findings in a timely manner.

2011 Ambysoft Survey of 178 respondents

Why agile? Higher success rates



Survey Results [Partial]



Source: 2010 How Agile Are You? Survey
www.ambysoft.com/surveys/
Copyright 2010 Scott W. Ambler

24th Annual
SSTC
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

Corporate Services as an Enabler

- Optimized **resource utilization**, which ***lowers overall capital expenditures***
- Greater **flexibility** through dynamic **resource allocation**
- Simple, **cost-effective** upgrades
- Homogeneous Security Platform
- *Reduced Development Cost*
- Support for **on-demand** usage models
- **Removes** common services like ***resource management*** and ***security*** *responsibilities* **from application code**
- Enables **reuse** of existing infrastructure services

24th Annual
SSTC
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

Agile Provisioning Services for Virtualized Security

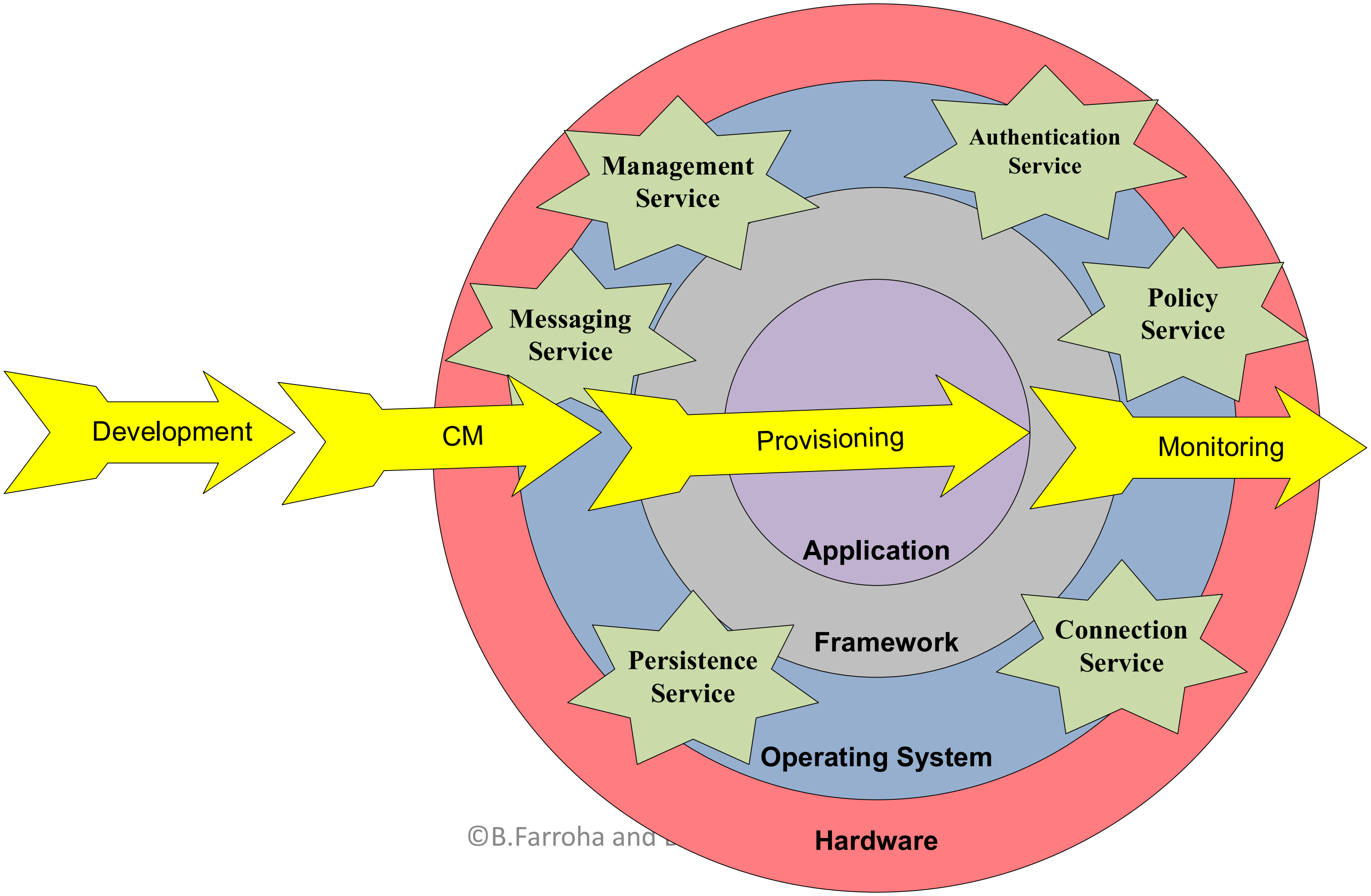
The attempt is to have all new applications leverage **common** services including **Security services** of the enterprise:

- The model has to support **ownership and control of sensitive data** and **tracking of access** by the data steward
- **Thin client** is the primary approach to **alleviating the client-server bottleneck paradigm.**
- Providing *different security roles* on a **per-user** and **per-service** basis ensures customization of client interactions. In other words, the stakeholder only **pays for what they need** in terms of performance and resources.
- ***Data Isolation*** has to be achieved using ***logical isolation*** methods, since the physical storage and processing are shared
- Identity, Authentication and other static and dynamic Attributes are used to grant Access right based on dynamic Digital Policy Management

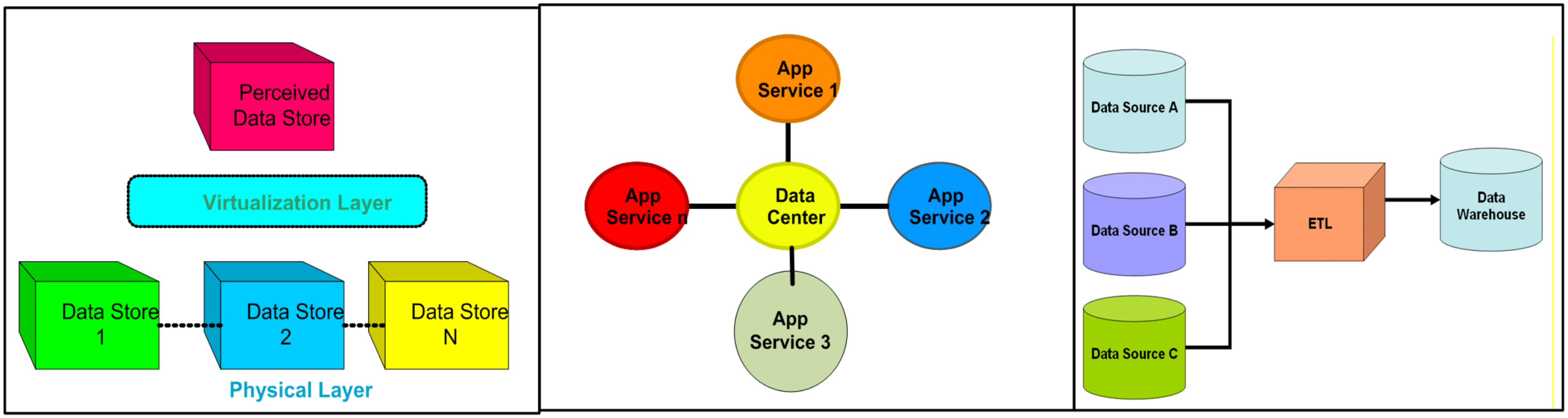
Agile Provisioning Services for Virtualized Security (cont)

- **Strong security** is needed for Positive identity and **access control**, as well as for **stronger encryption** and **key management**
- Use of **Open Source** enables sharing and leveraging resources, but may open up vulnerabilities
- **Leverage COTS** in new services
- **Cost** and performance can be **distributed** over the organizations utilizing the security services
- **Elastic** capabilities to **spur new processes** over the available ubiquitous computing resources
- **Ease of entry** by simply *subscribing* to the common service

Service-Based Architecture using a Security Framework

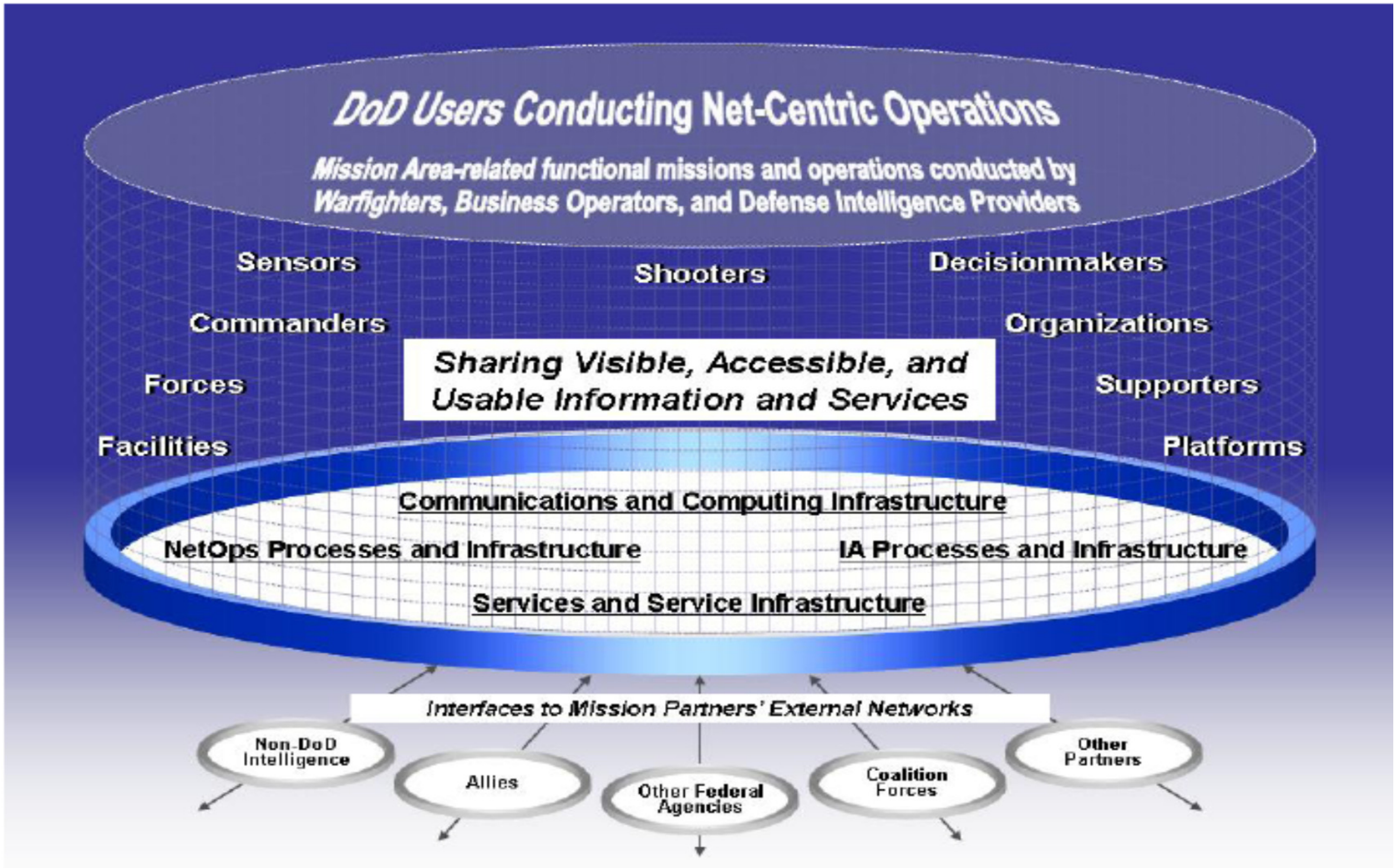


How do we Secure our Data when it Extends Globally?



Data Virtualization Constructs all relying on Data Services

Why we need an Agile Service-based Environment..



DoD Users Conducting Net-Centric Operations

Mission Area-related functional missions and operations conducted by Warfighters, Business Operators, and Defense Intelligence Providers

Sharing Visible, Accessible, and Usable Information and Services

Sensors
Shooters
Decisionmakers
Commanders
Organizations
Forces
Supporters
Facilities
Platforms
Communications and Computing Infrastructure
NetOps Processes and Infrastructure
IA Processes and Infrastructure
Services and Service Infrastructure
Interfaces to Mission Partners' External Networks
Non-DoD Intelligence
Allies
Other Federal Agencies
Coalition Forces
Other Partners

Deploying Automated Secure Systems in an SoS Environment

- **Detect**
  - This level of assurance ***can only be accomplished*** by providing a **continuous monitoring** capability to discover hostile actions and detect errors and attacks as soon as possible.
- **React**
  - The first action network administrators do upon **discovering security violations** is to **close security holes** and **isolate infected areas**.
- **Upgrade and Update**
  - **Subscribe to one of the leading malware detection and removal tools** to receive the most recent patches and methods and agile methods to apply the patches to all elements of the enterprise and ensure that there are no exposures and weak links that stay vulnerable
- **Predict and Invest**
  - **Technology trends ……. Adversary Trends ……. Industry trends**

Deploying Automated Secure Systems in an SoS Environment (cont)

- **Alternative Planning**
  - Ensure that we have **processes and development and maintenance** approaches to **recover data and systems once they have been attacked** and alternative resources to ensure continued operations (COOP) of the enterprise when the system is attacked and being recovered.
- **Meeting the Next Generation Capability needs**
  - The DoD and many leading commercial and governmental agencies are quickly developing and implementing plans to migrate to the a **cloud based environment** where services and/or data storage will be handled by **third parties** within or outside the enterprise.
  - This approach necessitates the development of ***agile methods*** to *deal with threats and attacks* quickly and *re-instantiate reliable services* to all stakeholders in an expedited manner.
  - **Agility in defending the identities, data, and services, is essential to protect the enterprise resources**

THE SECURITY FRAMEWORK for Agile Developers

[NIST Special Publication 800-53 Revision 3 on Information Security]

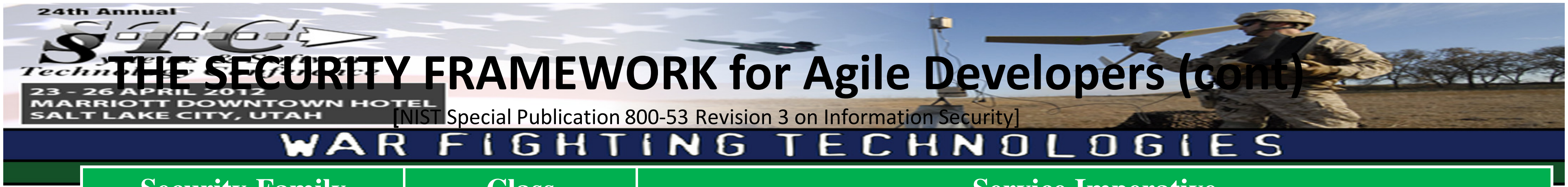
Security Family	Class	Service Imperative
Access Control	**Technical**	Institute an **authorization service** to authenticate user attributes and data classification.
		Ensure all data is **tagged appropriately** to enable sharing at the same classification or higher level.
		Institute an **integrity checking** mechanisms to ensure applications, data or users cannot access information they are not authorized or accredited to access.
		Ensure **appropriate blocking mechanisms** are in place to counter rogue applications or users.
Audit and Accountability	**Technical**	Institute an **automated audit logging** capability to capture all access, authentication, assertions and denial events.
		Ensure **audit reports are generated at a pre-defined tempo** and that they include metadata such as time stamps, identification data, adjudication information and out of bounds data.
		Institute an archival capability to save dated reports to enable forensic analysis to occur in the event of a security breach.
		Collect metrics on all security events to load balance security services.
Identification and Authentication	**Technical**	**Create a Public Key Infrastructure (PKI)** to make available to all applications to enable single sign-on, ensure privacy, provide authentication, maintain integrity and guarantee non-repudiation.
		Provide the ability to **enable reciprocity for authentication** between systems inside and outside the domain.
		Provide the ability to **uniquely identify individuals, devices and** applications to uphold integrity.

24th Annual
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

THE SECURITY FRAMEWORK for Agile Developers (cont)

[NIST Special Publication 800-53 Revision 3 on Information Security]

Security Family	Class	Service Imperative
System and Information Integrity	**Operational**	Leverage the authentication service to ensure **the right data is available to the right applications.**
		Ensure all **data is tagged appropriately** to enable sharing at the same classification or higher level.
		Institute an **integrity checking** mechanisms to *ensure applications, data or users cannot access information they are not authorized or accredited to access*.
		Institute data checking mechanisms to ensure the validity of the data as it is used by different applications.
		Log all metadata on data requests and transmission to capture data provenance to further ensure data integrity.



THE SECURITY FRAMEWORK for Agile Developers (cont)

[NIST Special Publication 800-53 Revision 3 on Information Security]

Security Family	Class	Service Imperative
System Communication and Protection	**Technical**	All **security services must be bounded and self contained** to maximize reusability and to avoid ambiguity with other non-security services.
		A sampling of **the type of attacks we want to detect through security monitoring** are as follows: **1.** **Malicious Code:** This is transmitted to the victim's site through Attachments, Piggybacking, Internet Worms, Web Browser Exploits, Hacking, and Affiliate Marketing. **2.** **Infiltration:** This includes social and technical infiltration of the information systems and the personnel managing these important assets. The adversary agents get access through physical or logical access holes in the security and steal, destroy and manipulate information. **3.** **Unauthorized Access:** This is the process by which an outsider gains access to a system or network, or an authorized person gains access at a higher level than he/she legitimately needs in order to take an unfair advantage of the system to destroy, damage, or transmit the information to an unauthorized user or for an unaccepted use. **4.** **Data Source/Results Corruption:** This type of attack is accomplished by attacking the information via malware or physical destruction of the system hosting the information. **5.** **Denial of Service (DOS):** This type of attack usually consists of the concerted efforts of a person or persons to prevent the information source services from functioning efficiently or at all, by temporarily or indefinitely flooding the servers with requests beyond their ability to respond.
		Monitor and log **metrics** to capture out of bounds data, communication links, data volume transmission and length of connection in order ***to guarantee availability, protect privacy and maintain the integrity of the system.***
		Institute c**hecking** mechanisms to ensure all data is tagged with the **appropriate security metadata**.
		Ensure any remote user, application or device is authenticated prior to access.

24th Annual
SSTC
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

Conclusions

- Building capabilities using a **service-based architecture** provides key benefits
  - System components are **discoverable**,
  - Services can be made **interoperable**, **loosely coupled** and **decentralized**
  - A **federated service-based** enables **heterogeneous data access** and **service interoperability** in a multi-organizational enterprise.
- **Information sharing through protected means and leveraging Agile methodologies** allows us **dynamically adjust to accommodate *Threats*** and National Security Strategy.
- Agility and Modularity play an increasingly important role in developing a COTS based Secure Enterprise
- Computing and Communication services are becoming a commodity, but securing them is still critical a tasks to gain the promised Efficiencies
- This framework **takes advantage of decades of system development** techniques **to arrive** at a **secure and flexible architecture** for the enterprise.
- The Framework is based on **developing security at project inception and using a Service based construct to leverage security as a service.**

24th Annual
SSTC
Systems & Software Technology Conference
23 - 26 APRIL 2012
MARRIOTT DOWNTOWN HOTEL
SALT LAKE CITY, UTAH
WAR FIGHTING TECHNOLOGIES
ENHANCE ADVANCE MODERNIZE

Contact Information

Dr. Bassam Farroha
Technical Director
Enterprise IA Architecture and Applications
Department of Defense
bassam.s.farroha@ugov.gov

Ms. Deborah L. Farroha
Technical Director
Enterprise Systems Engineering and Architecture
Department of Defense
Deborah.l.Farroha@ugov.gov